PACIFIC JOURNAL OF MATHEMATICS
Vol. 118, No 2, 1985

THE SET OF PRIMES DIVIDING THE LUCAS NUMBERS HAS DENSITY 2/3

J. C. LAGARIAS

Dedicated to the memory of Ernst Straus

The Lucas numbers L_n are defined by $L_0 = 2$, $L_1 = 1$ and the recurrence $L_n = L_{n-1} + L_{n-2}$. The set of primes $S_L = \{p: p \text{ divides } L_n \text{ for some } n\}$ has density 2/3. Similar density results are proved for sets of primes $S_U = \{p: p \text{ divides } U_n \text{ for some } n\}$ for certain other special second-order linear recurrences $\{U_n\}$. The proofs use a method of Hasse.

1. Introduction. There has been a good deal of study of the structure of the set of prime divisors of the terms $\{U_n\}$ of second order linear recurrences. M. Ward **[15]** showed that there are always an infinite number of distinct primes dividing the terms $\{U_n\}$, provided we exclude certain degenerate cases such as $U_n = 2^n$. In fact, under the same circumstances it is believed that the set of primes dividing the terms $U = \{U_n\}$ of any nondegenerate second order linear recurrence has a positive density $d(U)$ depending on the recurrence. This can be proved under the assumption that the Generalized Riemann Hypothesis is true by a method analogous to Hooley's conditional proof **[4]** of Artin's Conjecture for primitive roots. P. J. Stephens **[13]** has done this for a large class of second-order linear recurrences.

The point of this paper is that there are special second order linear recurrences where it is possible to give an unconditional proof of the existence of a density. This was shown by Hasse **[3]** for certain special second order linear recurrences having a reducible characteristic polynomial, in the process of solving a problem of Sierpinski **[12]**. Sierpinski's problem concerns the existence of a density for the set of primes p for which $\text{ord}_p 2$ is even. This set of primes is exactly the set of primes dividing some term of the sequence $V_n = 2^n + 1$; this sequence satisfies the reducible second order linear recurrence $V_n = 3V_{n-1} - 2V_{n-2}$ with $V_0 = 2$ and $V_1 = 3$.

THEOREM A. (*Hasse*) *The set of primes* $S_V = \{p: p$ *is prime and* p *divides* $2^n + 1$ *for some* $n \geq 0\}$ *has density* $17/24$.

Hasse's result [**3**] actually covers all the sequences $\{a^n + 1: n \geq 0\}$, where a is an integer, and the density of the associated set of primes is $2/3$ when $a \geq 3$ is squarefree.

Here we observe that Hasse's method with some extra complications extends to cover certain second-order linear recurrences with irreducible characteristic polynomials. The most interesting example of this phenomonon is the Lucas numbers L_n defined by $L_1 = 2$, $L_2 = 1$ and the recurrence $L_{n+1} = L_n + L_{n-1}$.

THEOREM B. *The set of primes* $S_L = \{ p$: *p is prime and p divides some Lucas number* $L_n\}$ *has density* $2/3$.

Theorem B also can be derived from polynomial-splitting criteria of M. Ward [**16**] for membership in S_L. The full proof is then essentially the same proof as given here.

The following recurrence discussed in Laxton [**8**] provides another interesting example.

THEOREM C. *Let* W_n *denote the recurrence defined by* $W_0 = 1$, $W_1 = 2$ *and* $W_n = 5W_{n-1} - 7W_{n-2}$. *Then the set* $S_W = \{ p$: *p is prime and p divides* W_n *for some* $n\}$ *has density* $5/8$.

The parameterized families of recurrences $A_n(m)$ and $B_n(m)$, both of which satisfy the recurrence

$$U_n = mU_{n-1} - U_{n-2}$$

with initial conditions $A_0(m) = B_0(m) = 1$ and $A_1(m) = m + 1$, $B_1(m) = m - 1$, are also recurrences to which Hasse's method applies. In the case that $\varepsilon = \frac{1}{2}(m + \sqrt{m^2 - 4})$ is the fundamental unit in $K = Q(\sqrt{m^2 - 4})$ the sets $S_A(m) = \{ p$: p is prime and p divides $A_n(m)$ for some $n\}$ and $S_B(m) = \{ p$: p is prime and p divides $B_n(m)$ for some $n\}$ each have density $1/3$. I omit the details.

In what circumstances is Hasse's method applicable? Any irreducible second-order recurrence $\{U_n\}$ whose terms U_n are rational numbers can be expressed in the form

$$U_n = \alpha\theta^n + \bar{\alpha}\bar{\theta}^n$$

where α and θ are in the quadratic field K generated by the roots of the characteristic polynomial of $\{U_n\}$, and $\bar{\alpha}$, $\bar{\theta}$ are the algebraic conjugates of α, θ in K. Hasse's method applies whenever:

(i) $\theta/\bar{\theta} = \pm\phi^k$ where $k = 1$ or 2 for some ϕ in K.

(ii) $\bar{\alpha}/\alpha = \zeta\phi^j$ where ζ is a root of unity in K and j is an integer. The actual densities of the sets of primes obtained depend in an idiosyncratic way on α and θ, which makes it awkward to state and prove a general result. For this reason I have applied the method to special cases. From the pattern of these proofs one should be able in principle to work out the density of a set of primes associated to any particular recurrence to which the method applies.

The proofs actually show that the sets of primes $S_U = \{p\colon p \text{ is prime and } p \mid U_n \text{ for some } n\}$ for these particular recurrences $\{U_n\}$ covered by Hasse's method have a special property. To state this property, we need some definitions. A set Σ of primes is a *Chebotarev set* if there is some finite normal extension L of the rationals Q such that a prime p is in Σ if and only if the Artin symbol

$$\left[\frac{L/Q}{(p)}\right]$$

is in specified conjugacy classes of the Galois group $\mathrm{Gal}(L/Q)$, cf. [**5**]. Chebotarev sets of primes Σ are guaranteed to have a natural density $d(\Sigma)$ given by the Chebotarev density theorem, cf. [**10**]. The special property is:

Property D. *Both the set S of primes and its complement $\bar{S} = \{p\colon p$ is prime and $p \notin S\}$ have a decomposition into disjoint countable unions of Chebotarev sets of primes. That is,*

$$S = \bigcup_{j=1}^{\infty} S^{(j)}, \qquad \bar{S} = \bigcup_{j=1}^{\infty} \bar{S}^{(j)}$$

where $S^{(j)}$ and $\bar{S}^{(j)}$ are Chebotarev sets. The densities of these sets satisfy

$$\sum_{j=1}^{\infty} d(S^{(j)}) + \sum_{j=1}^{\infty} d(\bar{S}^{(j)}) = 1.$$

It is easy to show that any set of primes S having property D has a natural density $d(S)$ given by

$$d(S) = \sum_{j=1}^{\infty} d(S^{(j)}).$$

For most second order recurrences $\{U_n\}$ the set of primes S_U associated to the recurrence is not known to have Property D, and probably it doesn't. However, it seems a difficult problem to show that there exists even one set S_U that doesn't have Property D. As a test case, does the set S_Y of primes dividing the terms of the recurrence given by $Y_n = Y_{n-1} + Y_{n-2}$ with $Y_0 = 3$ and $Y_1 = 1$ not have Property D?

I give a proof of Theorem A in §2 for comparison with the more involved details of the proofs of Theorem B and C in §§3 and 4, respectively.

2. Proof of Theorem A. The condition that $p | 2^n + 1$ for some n can be rewritten as:

$$2^n \equiv -1 \pmod{p} \text{ is solvable.} \tag{2.1}$$

Now let $m = \operatorname{ord}_p 2$, the least positive integer with

$$2^m \equiv 1 \pmod{p}. \tag{2.2}$$

Now (2.1) is solvable if and only if m is even and the smallest solution to (2.1) in that case is $n = \frac{1}{2}m$. Now suppose 2^j exactly divides $p - 1$. Then we have:

$$2^j \| p - 1 \text{ and } \operatorname{ord}_p 2 \text{ is odd} \Leftrightarrow 2^{(p-1)/2^j} \equiv 1 \pmod{p}. \tag{2.3}$$

Hasse observes that the condition on the right side of (2.3) is a splitting condition for primes in a certain algebraic number field K_j; such sets of primes have a density by the Frobenius density theorem.

Consequently we proceed by decomposing the set S_V into disjoint sets

$$S_V = \bigcup_{j=1}^{\infty} S_V^{(j)} \tag{2.4}$$

given by

$$S_V^{(j)} = \{ p : p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } p \in S_V \}.$$

We also define

$$\bar{S}_V^{(j)} = \{ p : p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } p \notin S_V \}.$$

and observe $p \in \bar{S}_V^{(j)}$ if and only if $p \equiv 1 + 2^j \pmod{2^{j+1}}$ and (2.3) holds. To state Hasse's observation precisely, let C_j denote the cyclotomic field $Q(\sqrt[2^j]{1})$, let $K_j = Q(\sqrt[2^j]{1}, \sqrt[2^j]{2})$ and let $L_j = Q(\sqrt[2^{j+1}]{1}, \sqrt[2^j]{2})$.

LEMMA 2.1. (1) *The primes p in* $\bar{S}_V^{(j)}$ *are exactly the primes p that split completely in* K_j *but not in* L_j.

(2) *The degree* $[K_j : Q]$ *is* 2, 8 *and* 2^{2j-2} *for* $j = 1$, $j = 2$ *and* $j \geq 3$, *respectively. The index* $[L_j K_j] = 2$ *except for* $j = 2$ *where* $K_2 = L_2$.

(3) *The primes p in* $\bar{S}_V^{(j)}$ *have densities* d_j^* *equal to* $1/4$, 0 *and* 2^{-2j+1} *for* $j = 1$, $j = 2$ *and* $j \geq 3$, *respectively. The primes p in* $S_V^{(j)}$ *have densities*

$d_j = 2^{-j} - d_j^*$ *for all* $j \geq 1$. *That is,*

$$\#\{p \leq x : p \in \bar{S}_V^{(j)}\} \sim d_j^* \frac{x}{\ln x},$$

$$\#\{p \leq x : p \in S_V^{(j)}\} \sim (2^{-j} - d_j^*)\frac{x}{\ln x},$$

as $x \to \infty$.

Proof. To prove (1) we observe that the fields $C_j = Q(\sqrt[2^{j-1}]{-1})$, $K_j = C_j(\sqrt[2^j]{2})$ and $L_j = C_{j+1}(\sqrt[2^j]{2})$ are all normal extensions of the rationals. The condition that the ideal (p) split completely over a cyclotomic field $Q(\sqrt[m]{1})$ is well known to be $p \equiv 1 \pmod{m}$ ([**2**], Lemma 4), hence $p \equiv 1 \pmod{2^j}$ holds if and only if p splits completely in C_j. The condition that a prime ideal p in C_j split completely in the Kummer extension $K_j = C_j(\sqrt[2^j]{2})$ is exactly that

$$x^{2^j} \equiv 2 \ (\mathrm{mod}\,(p)) \quad \text{for } x \in O_j \tag{2.5}$$

be solvable over the ring of integers O_j for C_j ([2], Lemma 5). If p is of degree 1 then any algebraic integer x in C_j is congruent to a rational integer (mod p) so in this case equation (2.5) is solvable if and only if

$$x^{2^j} \equiv 2 \pmod{p} \quad \text{for } x \in \mathbb{Z} \tag{2.6}$$

is solvable. By Euler's criterion (2.6) is solvable if and only if

$$2^{(p-1)/2^j} \equiv 1 \pmod{p} \tag{2.7}$$

is solvable. This is exactly (2.3), and we have shown (p) splits completely in K_j iff $p \equiv 1 \pmod{2^j}$ and (2.7) holds. Similarly (p) splits completely in L_j iff $p \equiv 1 \pmod{2^{j+1}}$ and (2.7) holds. This proves (1).

To prove (2), we first observe that $[C_j\colon Q] = \phi(2^j) = 2^{j-1}$. The special circumstance that $C_3 = Q(\sqrt[4]{-1}) = Q(\sqrt{-1}, \sqrt{2})$ shows that $K_2 = L_2 = Q(\sqrt{-1}, \sqrt[4]{2})$, and that $\alpha = \sqrt{2}$ is in C_j for $j \geq 3$. The fact that $K_2 = C_2(\sqrt[4]{2})$ is a nonabelian extension of Q guarantees that $\sqrt[4]{2}$ is not in any of the abelian extensions C_j. Now observe that $K_j = C_j(\sqrt[2^{j-1}]{\alpha})$ for $j \geq 3$ is a Kummer extension so that $[K_j : C_j]$ divides 2^{j-1}. In fact for $j \geq 3$ α is of order 2^k in $C_j^*/(C_j^*)^{2^k}$ for any k because $\sqrt[4]{2}$ isn't in C_j, hence using [**2**], Lemma 1 we have $[K_j : C_j] = 2^{j-1}$ for $j \geq 3$ and also $[L_j : C_{j+1}] = 2^{j-1}$ for $j \geq 3$ using $L_j = C_{j+1}(\sqrt[2^{j-1}]{\alpha})$. Thus $[K_j : Q] = [K_j : C_j][C_j : Q] = 2^{2j-1}$ for $j \geq 3$ and $[L_j : Q] = 2^{2j-1}$ for $j \geq 3$ so that $d_j^* = 2d_j$ for $j \geq 3$. Finally one checks that $[K_1' \colon Q] = 2$, $[L_1 : Q] = 4$ and $[K_2 : Q] = 8$, to prove (2).

To prove (3) we observe that for a normal extension K/Q of degree $[K:Q]$ the set of primes p that split completely in K has density $[K:Q]^{-1}$, which is a consequence of the prime ideal theorem (e.g. [**6**], p. 315 Theorem 4), a special case of both the Frobenius and Chebotarev density theorems. Thus using (1) we find that the set of primes in $\bar{S}_V^{(j)}$ is the difference of a set of primes of density $[K_j:Q]^{-1}$ less a class of primes contained in it of density $[L_j:Q]^{-1}$. Using (2) we compute this density d_j^* to be equal to $1/4$, 0 and 2^{-2j+1} for $j=1, j=2$ and $j \geq 3$, respectively. Finally the primes in $S_V^{(j)}$ are the difference of the class of primes $\{p \equiv 1 + 2^j \pmod{2^{j+1}}\}$ of density $2^{-j} = [C_j:Q]^{-1} - [C_{j+1}:Q]^{-1}$, and the class of primes $\bar{S}_V^{(j)}$ of density d_j^* contained in it. This proves (3). □

To complete the proof of Theorem A, we observe that for any fixed $m \geq 3$,

$$\bigcup_{j=1}^{m} S_V^{(j)} \subseteq S_V \subseteq \mathbf{P} - \bigcup_{j=1}^{m} \bar{S}_V^{(j)}$$

where $\mathbf{P}$ denotes the set of all primes. Using (3) of Lemma 2.1, the first inclusion gives

$$\#\{p \leq x : p \in S_V\} \geq \left(\frac{17}{24} - 2^{-m} - \frac{4}{3}2^{-2m+1}\right)\frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right)$$

as $x \to \infty$, since all the $S_V^{(j)}$ are disjoint. The second inclusion gives

$$\#\{p \leq x : p \in S_V\} \leq \left(\frac{17}{24} + \frac{4}{3}2^{-2m+1}\right)\frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right).$$

as $x \to \infty$. Letting $m \to \infty$ shows that

$$\#\{p \leq x : p \in S_V\} \sim \frac{17}{24}\frac{x}{\ln x}.$$

REMARKS. (1) By a careful analysis of error terms in this argument using an effective version of the Chebotarev density theorem, Odoni [**11**] has proved the stronger result that:

$$\#\{p \leq x : p \in S_V\} = \frac{17}{24}\operatorname{Li}(x) + O\left(Li(x)\exp\left(-c\frac{\ln\ln x}{\ln\ln\ln x}\right)\right)$$

where $\operatorname{Li}(x) = \int_2^x dt/\ln t$.

(2) The sets $S_V^{(j)}$ are sets of primes determined by systems of polynomial congruences in the sense of [**5**, Theorems 1.1 and 1.2].

3. Proof of Theorem B. The Lucas numbers L_n satisfy

$$L_n = \varepsilon^n + \bar{\varepsilon}^n \tag{3.1}$$

where

$$\varepsilon = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \bar{\varepsilon} = \frac{1-\sqrt{5}}{2}.$$

Hence

$$(3.2) \qquad p \mid L_n \Leftrightarrow \varepsilon^n + \varepsilon^{-n} \equiv 0 \,(\mathrm{mod}(p)) \Leftrightarrow \theta^n \equiv -1 \,(\mathrm{mod}\,(p))$$

where

$$\theta = \frac{\varepsilon}{\bar{\varepsilon}} = -\varepsilon^2 = -\frac{3+\sqrt{5}}{2}$$

and the congruences are in the ring $\mathbb{Z}[(1+\sqrt{5})/2]$ of algebraic integers in $Q(\sqrt{5})$. Thus S_L is exactly the set of primes p for which the exponential congruence over $\mathbb{Z}[(1+\sqrt{5})/2]$ given by

$$(3.3) \qquad \theta^x \equiv -1 \,(\mathrm{mod}(p))$$

is solvable for some integer x.

We now proceed analogously to the proof of Theorem A. We must treat several cases according to the behavior of the ideal (p) in $\mathbb{Z}[(1+\sqrt{5})/2]$. If $p \equiv \pm 1 \pmod 5$ then $(p) = \pi\bar{\pi}$ splits into two conjugate degree 1 prime ideals, while if $p \equiv \pm 2 \pmod 5$ then (p) is a degree 2 prime ideal in $\mathbb{Z}[(1+\sqrt{5})/2]$. Let $S_L = S_A \cup S_B$ where

$$S_A = \{p : p \in S_L \text{ and } p \equiv \pm 1 \pmod 5\}$$

and

$$S_B = \{p : p \in S_L \text{ and } p \equiv \pm 2 \pmod 5\}.$$

Case 1. The primes in S_A have density $5/12$.

Write $(p) = \pi\bar{\pi}$ in $\mathbb{Z}[(1+\sqrt{5})/2]$. In this case (3.3) is equivalent to

$$(3.4) \qquad \theta^x \equiv -1 \,(\mathrm{mod}\,\pi)$$

being solvable. To see this, suppose (3.4) holds and apply the automorphism taking $\sqrt{5}$ to $-\sqrt{5}$ to (3.4) to get

$$(3.5) \qquad \bar{\theta}^x \equiv -1 \,(\mathrm{mod}\,\bar{\pi}).$$

Since $\theta\bar{\theta} = 1$ we have $\theta^x\bar{\theta}^x = 1$ so (3.5) implies

$$\theta^x \equiv -1 \,(\mathrm{mod}\,\bar{\pi}).$$

Combining this with (3.4) shows (3.3) holds. The reverse direction is clear.

Now we have the equivalence

$$(3.6) \qquad \mathrm{ord}_{\pi_1}\theta \text{ is even} \Leftrightarrow \theta^x \equiv -1 \,(\mathrm{mod}\,(p)) \text{ is solvable}.$$

If $p \equiv 1 + 2^j \pmod{2^{j+1}}$ we obtain

$$2^j \| p - 1 \quad \text{and} \quad \operatorname{ord}_\pi \theta \text{ is odd} \Leftrightarrow \theta^{(p-1)/2^j} \equiv 1 \pmod{\pi}.$$

This leads us to split S_A into the disjoint union of sets

$$S_A = \bigcup_{j=1}^{\infty} S_A^{(j)},$$

where

$$S_A^{(j)} = \left\{ p : p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } \operatorname{ord}_\pi \theta \text{ is even} \right\}.$$

We set

$$\bar{S}_A^{(j)} = \left\{ p : p \equiv 1 + 2^j \pmod{2^{j+1}} \text{ and } \operatorname{ord}_{\pi_1} \theta \text{ is odd} \right\}.$$

The associated fields are

$$K_j^* = Q\left(\sqrt[2^j]{1}, \sqrt{5}, \sqrt[2^j]{\theta}\right) \quad \text{and} \quad L_j^* = Q\left(\sqrt[2^{j+1}]{1}, \sqrt{5}, \sqrt[2^j]{\theta}\right).$$

LEMMA 3.1. (1) *$\bar{S}_A^{(1)}$ is empty. For $j \geq 2$ the primes p in $\bar{S}_A^{(j)}$ are exactly the primes that split completely in K_j^* and which do not split completely in L_j^*.*

(2) *The primes in $\bar{S}_A^{(1)}$ and $S_A^{(1)}$ have densities* 0 *and* $1/4$, *respectively. For $j \geq 2$ the primes in $\bar{S}_A^{(j)}$ have density 2^{-2j} and those in $S_A^{(j)}$ have density $2^{-j-1} - 2^{-2j}$.*

Proof. Similar to that of Lemma 2.1. The relation $\theta = -\varepsilon^2$ leads to $K_1^* = L_1^* = Q(\sqrt{-1}, \sqrt{5})$; this causes $\bar{S}_A^{(1)}$ to be empty. For $j \geq 2$ one checks that $[K_j^* : Q] = 2^{2j-1}$ and $[L_j^* : Q] = 2^{2j}$. In fact for $j \geq 2$, $K_j^* = Q(\omega_j, \sqrt{5}, \phi_{j-2}, \sqrt{\omega_j \phi_{j-2}})$ where $\omega_j = \sqrt[2^{j-1}]{-1}$ and $\psi_{j-2} = \sqrt[2^{j-2}]{\varepsilon}$, and $L_j^* = Q(\omega_{j+1}, \sqrt{5}, \phi_{j-1})$. Finally note that the set $S_A^{(j)} \cup \bar{S}_A^{(j)} = \{ p : p \equiv \pm 1 \pmod 5\}$ and $p \equiv 1 + 2^j \pmod{2^{j+1}}$ has density 2^{-j-1}. □

As in the proof of Theorem A we find the primes in S_A have density $\frac{1}{4} + \sum_{j=2}^{\infty}(2^{-j+1} - 2^{-2j}) = \frac{5}{12}$.

Case 2. The primes in S_B have density $1/4$.

The primes $p \equiv \pm 2 \pmod 5$ remain inert in $\mathbb{Z}[(1 + \sqrt{5})/2]$, and in this case

$$\theta^x \equiv -1 \pmod{(p)} \text{ is solvable} \Leftrightarrow \operatorname{ord}_{(p)} \theta \text{ is even}.$$

Now

$$(3.7) \qquad \theta^{(p+1)/2} = (-1)^{(p+1)/2}\varepsilon^{p+1} \equiv a \pmod{p}$$

for some $a \in \mathbb{Z}$ because $GF(p)^* = \{\psi^{p+1}: \psi \in GF(p^2)^*\}$. Applying the nontrivial automorphism of $Q(\sqrt{5})$ gives

$$\bar{\theta}^{(p+1)/2} \equiv a \pmod{p}$$

hence

$$1 = (\theta\bar{\theta})^{(p+1)/2} \equiv a^2 \pmod{(p)}.$$

Thus

$$(3.8) \qquad \theta^{p+1} \equiv a^2 \equiv 1 \pmod{(p)}$$

Consequently $\operatorname{ord}_{(p)} \theta \mid p + 1$. Now when $p \equiv -1 + 2^j \pmod{2^{j+1}}$ we have

$$(3.9) \qquad \theta^{(p+1)/2^j} \equiv 1 \pmod{(p)} \Leftrightarrow \operatorname{ord}_{(p)} \theta \text{ is odd.}$$

We now decompose

$$S_B = \bigcup_{j=1}^{\infty} S_B^{(j)}$$

where

$$S_B^{(1)} = \{p : p \equiv 1 \pmod 4 \text{ and } p \in S_B\}.$$

and for $j \geq 2$

$$S_B^{(j)} = \{p : p \equiv -1 + 2^j \pmod{2^{j+1}} \text{ and } p \in S_B\}.$$

We complete case 2 with the following lemma.

LEMMA 3.2. (1) *$S_B^{(1)}$ is empty.*

(2) *For $j \geq 2$ all $S_B^{(1)} = \{p:\ p \equiv -1 + 2^j \pmod{2^{j+1}}$ and $p \equiv \pm 2 \pmod 5)\}$ and $S_B^{(j)}$ has density 2^{-j-1}.*

Proof. (1) When $j = 1$ we have

$$(3.10) \qquad \theta^{(p+1)/2} \equiv 1 \pmod{(p)} \Leftrightarrow \operatorname{ord}_{(p)} \theta \text{ is odd.}$$

Now $\theta = -\varepsilon^2$ so

$$(3.11) \qquad \theta^{(p+1)/2} \equiv (-\varepsilon^2)^{(p+1)/2} \equiv -\varepsilon^{p+1} \pmod{(p)}.$$

We claim that

$$\varepsilon^{p+1} \equiv -1 \pmod{(p)}$$

which with (3.11) shows $\theta^{(p+1)/2} \equiv 1 \pmod{(p)}$ and so by (3.10) $\operatorname{ord}_p \theta$ is odd and $S_B^{(1)}$ is empty.

To prove the claim, set

$$\varepsilon^{(p+1)/2} \equiv \phi \pmod{(p)}$$

so that

$$\varepsilon^{p+1} \equiv \phi^2 \pmod{(p)}. \tag{3.12}$$

By algebraic conjugation $\bar{\varepsilon}^{(p+1)/2} \equiv \bar{\phi} \pmod{p}$ and $\varepsilon\bar{\varepsilon} = -1$ so that

$$-1 = (-1)^{(p+1)/2} \equiv (\varepsilon\bar{\varepsilon})^{(p+1)/2} \equiv \phi\bar{\phi} \pmod{(p)}. \tag{3.13}$$

By (3.8) $\varepsilon^{p+1} \equiv \pm 1 \pmod{(p)}$. We suppose that $\varepsilon^{p+1} \equiv 1 \pmod{(p)}$ and get a contradiction. In that case (3.12) gives $\phi^2 \equiv 1 \pmod{(p)}$, hence $\phi \equiv \pm 1 \pmod{(p)}$. Hence $\phi \equiv \bar{\phi} \pmod{(p)}$ and (3.13) now gives

$$\phi^2 \equiv -1 \pmod{(p)},$$

the desired contradiction.

(2) We must show that in the case $j \geq 2$ $\operatorname{ord}_{(p)} \theta$ is even for any $p \equiv -1 + 2^j \pmod{2^{j+1}}$ and $p \equiv \pm 2 \pmod 5$. We argue by contradiction. Suppose $\operatorname{ord}_{(p)} \theta$ were odd, so that by (3.8) we have

$$\theta^{(p+1)/2^j} \equiv 1 \pmod{(p)}. \tag{3.14}$$

Set

$$\varepsilon^{(p+1)/2^j} \equiv \phi \pmod{(p)}$$

and observe $\theta = -\varepsilon^2$ and (3.14) give

$$-\phi^2 \equiv 1 \pmod{(p)}. \tag{3.15}$$

Now

$$\bar{\varepsilon}^{(p+1)/2^j} \equiv \bar{\phi} \pmod{(p)}$$

and

$$-1 = (-1)^{(p+1)/2^j} \equiv (\varepsilon\bar{\varepsilon})^{(p+1)/2^j} \equiv \phi\bar{\phi} \pmod{(p)}. \tag{3.16}$$

Now by (3.15) $\phi^2 \equiv -1 \pmod{(p)}$ and since $p \equiv 3 \pmod 4$ we have $\bar{\phi} \equiv -\phi \pmod{(p)}$. Hence $\phi\bar{\phi} \equiv -\phi^2 \equiv 1 \pmod{(p)}$, contradicting (3.16). $\square$

As in the proof of Theorem A Lemma 3.2 implies the density of primes in S_B is $\sum_{j=2}^{\infty} 2^{-j-1} = 1/4$. This proves Theorem B. $\square$

Remark. It is possible to prove that

$$\#\{p \leq x : p \in S_L\} = \frac{2}{3} \operatorname{Li}(x) + O\left(\operatorname{Li}(x) \exp\left(-c \frac{\ln\ln x}{\ln\ln\ln x}\right)\right)$$

by the method of Odoni [**11**].

4. Proof of Theorem C (Sketch). We have

$$V_n = \left(\frac{1}{2} + \frac{1}{6}\sqrt{-3}\right)\left(\frac{5}{2} + \frac{1}{2}\sqrt{-3}\right)^n + \left(\frac{1}{2} - \frac{1}{6}\sqrt{-3}\right)\left(\frac{5}{2} - \frac{1}{2}\sqrt{-3}\right)^n. \tag{4.1}$$

Letting $\alpha = \frac{1}{2} + \frac{1}{6}\sqrt{-3}$ and $\gamma = \frac{5}{2} + \frac{1}{2}\sqrt{-3}$ we have

$$V_n \equiv 0 \ (\mathrm{mod}(p)) \Leftrightarrow \phi^n \equiv \frac{\bar{\alpha}}{\alpha} \ (\mathrm{mod}(p)), \tag{4.2}$$

where

$$\phi = \frac{\gamma}{\bar{\gamma}} = \frac{11 + 5\sqrt{-3}}{14} \quad \text{and} \quad -\frac{\bar{\alpha}}{\alpha} = \frac{-1 + \sqrt{-3}}{2}$$

is a cube root of unity. Hence (4.1) gives

$$p \text{ divides } V_n \text{ for some } n \geq 0 \Leftrightarrow \mathrm{ord}_{(p)}\, \phi \equiv 0 \ (\mathrm{mod}\ 3). \tag{4.3}$$

We consider separately the cases in which (p) splits completely or remains inert in $Q(\sqrt{-3})$.

Case 1. $p \equiv 1 \ (\mathrm{mod}\ 3)$.

Then $(p) = \pi\bar{\pi}$ in $\mathbb{Z}[(1 + \sqrt{-3})/2]$. Now as in Theorem B we have

$$\mathrm{ord}_{(p)}\, \phi \equiv 0 \ (\mathrm{mod}\ 3) \Leftrightarrow \mathrm{ord}_{\pi}\, \phi \equiv 0 \ (\mathrm{mod}\ 3), \tag{4.4}$$

using the fact that $\phi\bar{\phi} = 1$. Now let $3^j \| p - 1$, and observe that in this case

$$\mathrm{ord}_{\pi}\, \phi \not\equiv 0 \ (\mathrm{mod}\ 3) \Leftrightarrow \phi^{(p-1)/3^j} \equiv 1 \ (\mathrm{mod}\ \pi). \tag{4.5}$$

Then

$$\begin{aligned} \theta^{(p-1)/3^j} \equiv 1 \ (\mathrm{mod}\ \bar{\pi}) &\Leftrightarrow \pi \text{ splits completely in} \\ &\quad F_j = Q\left(\sqrt[3^j]{1}, \sqrt[3^j]{\theta}\right)/Q\left(\sqrt[3]{1}\right) \\ &\Leftrightarrow (p) \text{ splits completely in } F_j/Q. \end{aligned} \tag{4.6}$$

Hence the density of primes satisfying (4.6) is $[F_j : Q]^{-1} = (2 \cdot 3^{2j-1})^{-1}$, and the density d_j of primes with $3^j \| p - 1$ and (4.4) holding is

$$d_j = 2(2 \cdot 3^j)^{-1} - (2 \cdot 3^{2j-1})^{-1}.$$

The total contribution of such primes has density

$$D_1 = \sum_{j=1}^{\infty} d_j = \frac{5}{16}. \tag{4.7}$$

Case 2. $p \equiv 2 \pmod 3$.

Then (p) is inert in $\mathbb{Z}[(1+\sqrt{-3})/2]$ and as in Theorem B we have

$$\phi^{p+1} \equiv 1 \ (\mathrm{mod}(p))$$

and if $3^j \| p+1$ then

$$\mathrm{ord}_{(p)} \phi \not\equiv 0 \ (\mathrm{mod}\, 3) \Leftrightarrow \phi^{(p-1)/3^j} \equiv 1 \ (\mathrm{mod}\,(p)).$$

Now we have

$$\phi^{(p+1)/3^j} \equiv 1 \ (\mathrm{mod}(p)) \Leftrightarrow p \equiv 2 \ (\mathrm{mod}\, 3) \text{ and } (p) \text{ splits completely in } F_j/Q(\sqrt{-3}). \tag{4.8}$$

We claim that the set of primes defined by the right side of (4.8) has density $(2 \cdot 3^{2j-1})^{-1}$. To verify this, one checks that F_j/Q is Galois over Q with dihedral Galois group of order $2 \cdot 3^{2j-1}$, that the splitting condition (4.8) on primes in F_j/Q corresponds exactly to the Artin symbol

$$\left[\frac{F_j/Q}{(p)}\right]$$

being the conjugacy class $\langle \sigma \rangle$, where σ is the unique element of order two in $\mathrm{Gal}(F_j/Q)$. Then the Chebotarev density theorem implies that the set of primes in (4.8) has density $[F_j : Q]^{-1} = (2 \cdot 3^{2j-1})^{-1}$, as claimed.

Hence the density d_j^* of primes with $3^j \| p+1$ and (4.4) holding is

$$d_j^* = 2(2 \cdot 3^j)^{-1} - (2 \cdot 3^{2j-1})^{-1}$$

and the total density of such primes is

$$D_2 = \sum_{j=1}^{\infty} d_j^* = \frac{5}{16}. \qquad \square$$

Acknowledgments. I am indebted to J. P. Serre for informing me of the work of Hasse, and to C. Pomerance for helpful comments.

References

[1] A. Aigner, *Bemerkung und Lösung zum Problem* 29, Elem d. Math., **15** (1960), 66–67.

[2] B. J. Birch, *Cyclotomic Fields and Kummer Extensions*, in: *Algebraic Number Fields* (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, London 1967, 85–93.

[3] H. H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von gerader bzw. ungerader Ordung* mod *p ist.*, Math. Annalen, **168** (1966), 19–23.

[4] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math., **225** (1967), 209–220.

[5] J. C.. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math., **27** (1983), 224–235.

[6] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publ. Co., New York 1970.

[7] R. R. Laxton, *On groups of linear recurrences I*, Duke Math. J., **26** (1969), 721–736.

[8] _____, *On groups of linear recurrences II. Elements of Finite Order*, Pacific J. Math., **32** (1970), 173–179.

[9] _____, *Arithmetic Properties of Linear Recurrences*, in: *Computers and Number Theory* (A. O. L. Atkin and B. J. Birch, Eds.), Academic Press, New York, 1971, 119–124.

[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw 1974.

[11] R. W. K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory, **13** (1981), 303–319.

[12] W. Sierpinski, *Sur une decomposition des numbers premiers en deux classes*, Collect. Math., **10** (1958), 81–83. (Also: Problem 29, Elem. d. Math., **14** (1959), 60.)

[13] P. J. Stephens, *Prime divisors of second order linear recurrences I.*, J. Number Theory **8** (1976), 313–332.

[14] _____, *Prime divisors of second order linear recurrences II*, J. Number Theory, **8** (1976), 333–345.

[15] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 178–188.

[16] _____, *The prime divisors of Fibonacci numbers*, Pacific J. Math., **11** (1961), 379–386.

Received September 12, 1984 and in revised form September 28, 1984.

AT & T BELL LABORATORIES
MURRAY HILL, NJ 07974